UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

JEREMY HAMMOND,
a/k/a "Anarchaos,"
a/k/a "sup_g,"
a/k/a "burn,"
a/k/a "yohoho,"
a/k/a "POW,"
a/k/a "tylerknowsthis,"
a/k/a "crediblethreat,"
a/k/a "ghost," and
a/k/a "anarchacker,"

Defendant.

S2 12 Cr. 185 (LAP)

GOVERNMENT'S MEMORANDUM OF LAW WITH RESPECT TO SENTENCING

PREET BHARARA
United States Attorney for the
Southern District of New York

Attorney for the United States
of America

THOMAS BROWN
ROSEMARY NIDIRY
Assistant United States Attorneys
Of Counsel

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

JEREMY HAMMOND,
a/k/a "Anarchaos,"
a/k/a "sup_g,"
a/k/a "burn,"
a/k/a "yohoho,"
a/k/a "POW,"
a/k/a "tylerknowsthis,"
a/k/a "crediblethreat,"
a/k/a "ghost," and
a/k/a "anarchacker,"

Defendant.

S2 12 Cr. 185 (LAP)

The Government respectfully submits this memorandum in advance of the sentencing of Jeremy Hammond ("Hammond" or the "defendant"), which is scheduled for November 15, 2013 at 10:00 a.m. In his plea agreement with the Government (the "Plea Agreement"), Hammond has stipulated that the applicable United States Sentencing Guidelines ("Guidelines" or "U.S.S.G.") range would be 151 to 188 months' imprisonment but, in light of the statutory maximum of the offense of conviction, that his Guidelines sentence is 120 months' imprisonment. In its Presentence Investigation Report ("PSR"), the United States Probation Office ("Probation Office"), consistent with the Plea Agreement, recommends a sentence of 120 months.

Contrary to the picture he paints of himself in his sentencing submission, Hammond is a computer hacking recidivist who, following a federal conviction for computer hacking, went on to engage in a massive hacking spree during which he caused harm to numerous businesses,

individuals, and governments, resulting in losses of between $1 million and $2.5 million, and threatened the safety of the public at large, especially law enforcement officers and their families.

For the reasons set forth below, given the nature and circumstances of Hammond's outrageous and widespread cyber attacks, his history and characteristics, including the fact that he committed the instant offense conduct after having been previously convicted of closely similar criminal hacking, and the need to promote respect for the law and ensure just punishment, the Government submits that a stipulated Guidelines sentence of 120 months is entirely appropriate in this case.

BACKGROUND

I. Hammond's Offense Conduct

Hammond was a prolific and technically skilled hacker who launched cyber attacks against scores of governmental institutions, law enforcement organizations, and businesses during a nearly year-long rampage. Hammond's aim was to break into victims' computer systems, steal data, deface websites, destroy files and dump online the sensitive personal and financial information of thousands of individuals – all with the object of creating, in Hammond's own words, maximum "mayhem." (*See, e.g.*, Bates # 63161-62, 63172.) Between June 2011 and March 2012, when he was identified and arrested, Hammond attacked computer networks belonging to victims around the world. Evidence of Hammond's hacking spree came from online chats recorded by a cooperating witness (the "CW"), in which Hammond described his computer attacks; from victims; and from Hammond's laptop, which he was using at the moment

of his arrest to hack into at least one victim's computer network and which contained a trove of electronic files that not only corroborated several of the hacks he described to his co-conspirators and the CW, but also revealed that Hammond had engaged in many more attacks than previously known.

A. The Arizona Department of Public Safety Hack[1]

In June 2011– just weeks after Hammond's term of supervised release had ended on May 20, 2011, following his two-year term of imprisonment for a conviction on a federal computer hacking charge (PSR ¶¶ 60-63) – Hammond contacted the CW, who was a member of the Anonymous-affiliated hacking group LulzSec. In the preceding months, members of LulzSec had hacked into the computer systems of a number of governmental and business organizations around the world and had publicly dumped online stolen data in a series of high-profile "press releases," generating significant press attention. In subsequent conversations with the CW, Hammond said that he had stolen a large number of confidential law enforcement documents from the Arizona Department of Public Safety ("AZDPS"), including training manuals, private emails, and other sensitive data; provided samples of these documents; and sought LulzSec's assistance in publicly releasing the full set of stolen data in a similarly high profile manner.[2] (Bates # 78130-64.) Hammond told the CW that "black hats [criminal hackers]

---

[1] In the Plea Agreement, Hammond admitted the Arizona Department of Public Safety hack as relevant conduct to be considered at the time of his sentencing. (Plea Agreement at 1.)

[2] Upon learning that AZDPS's computer systems had been compromised, the FBI immediately notified AZDPS, as it did each time it received notice that Hammond or his co-conspirators had compromised an entity's computer systems.

need to unite especially going against police and the government,"[3] that he had a "three punch knockout plan" to dump the information on the Internet, and that he would write at least the first press release. (Bates # 78162, 78185, 78218, 78240.)

On June 23, 2011, members of LulzSec, including Mustafa al Bassam, a/k/a "Tflow" and Jake Davis, a/k/a "Topiary," publicized "Chinga La Migra [Fuck the Border Police] Bulletin #1," LulzSec's public release of numerous sensitive law enforcement documents that Hammond had stolen from AZDPS computer servers, along with the personal details of Arizona law enforcement officers – and their spouses – including names, email accounts and passwords, home addresses, cell phone numbers, and home phone numbers. (*See, e.g.*, Bates # 78197, 78199, 78213-14, 78246-47.) Over the next two weeks, "Operation Anti-Security" or "AntiSec," a new Anonymous-affiliated group that succeeded LulzSec, completed Hammond's "three punch knockout plan" by releasing "Chinga La Migra II" and "Chinga La Migra III," each of which contained additional sensitive Arizona law enforcement data and law enforcement officers' personal information, including information stolen from computer systems used by the Arizona Fraternal Order of Police.[4]

---

[3] The text of the chats is reproduced here as it appears in the chat logs; errors in spelling and punctuation have not been corrected.

[4] Indeed, the following note was found on Hammond's laptop: "[the Arizona Fraternal Order of Police's website] <-- we already owned 6 months ago but we can own again for lulz." Significantly, at least one core member of LulzSec was profoundly disturbed by the invasiveness and purposelessness of Hammond's attack on AZDPS and online dump of confidential and sensitive law enforcement data and personal information about police officers and their families. In an interview with the BBC in May 2013 following his conviction and sentence in the United Kingdom on charges related to his LulzSec activities, Jake Davis confessed that the "Chinga La Migra" data dump on June 23, 2011 was a "turning point" for him: "I thought this hack [of

B. The Stratfor, California Statewide Law Enforcement Association, New York State Association of Chiefs of Police and Special Forces Gear Hacks[5]

In December 2011, Hammond took over, organized and led a cyber attack against Strategic Forecasting, Inc. ("Stratfor"), a private intelligence firm based in Texas. During the course of that attack, Hammond (1) stole at least 200 gigabytes[6] of confidential information from Stratfor's computer systems, including the content of Stratfor employees' emails, account information relating to approximately 860,000 Stratfor clients, approximately 60,000 credit cards numbers belonging to Stratfor clients, and internal Stratfor corporate documents, including company financial data; (2) caused that information to be publicly disclosed; (3) defaced the Stratfor website; and (4) deleted all of the data on Stratfor's computer servers, effectively destroying the company. (PSR ¶ 15.) Hammond's criminal associates made at least $700,000 worth of unauthorized charges using the credit card information stolen and distributed by Hammond. (PSR ¶ 28.)

Hammond first learned about Stratfor from the CW on December 5, 2011. The CW told Hammond that another hacker, who used the online alias "hyrriiya," had said he had hacked the

---

AZDPS] has gone way too far – there's no point to this thing. It's just harming police officers . . . This doesn't entertain anybody or help anybody anywhere." *See* http://www.bbc.co.uk/news/technology-22526021.

[5] As described *infra*, Hammond pleaded guilty before Your Honor to the Stratfor hack. In the Plea Agreement, Hammond also admitted to the Special Forces Gear hack (among others) and agreed that it could be considered as relevant conduct at the time of his sentencing. (Plea Agreement at 2.) He did not admit the California Statewide Law Enforcement Association or New York State Association of Chiefs of Police hacks at his guilty plea.

[6] A gigabyte is a measure of data storage equivalent to approximately 675,000 pages of text.

company.[7] (Bates # 63691, 67014.) After further examination, Hammond determined that "hyrriiya" had gained only limited access to Stratfor's servers and not enough to exercise control over Stratfor's computer network.[8] (Bates # 67014 ("It looks like he needs help breaking into their servers.").) After telling the CW, "I want to sink my teeth into this stratfor.com target" (Bates # 67015), Hammond quickly took over the job of hacking Stratfor. Nine days later, on December 14, 2011, Hammond announced to a co-conspirator that he had "rooted," *i.e.*, gained complete access to, Stratfor's computer network:

[Hammond]	we in business baby
<@uid0>	w00t?
[Hammond]	oh yes
[Hammond]	time to feast upon their spools [email archives]
<@uid0>	stratfor?
[Hammond]	oh yes
[Hammond]	after yall left yesterday I spent another eight hours
[Hammond]	and rooted that mofo
<@uid0>	They're so done now . . .
[Hammond]	Yeah it's over with

---

[7] The FBI immediately notified Stratfor upon learning in early December that Stratfor's computer systems had been compromised. The FBI continued to provide updates to Stratfor as it learned more about Hammond's continued attack against that company.

[8] Indeed "hyrriiya" admitted as much in a conversation with Hammond:

[Hammond]	and then we have nothing for core.stratfor.com yet right?
<@hyrriiya>	we have that mysql [a database] and that is it

(Bates # 60801.)

(Bates # 63167.)

In further online conversations with his criminal associates, Hammond assumed leadership of how the hack would be exploited. For example, in a chat on December 19, 2011, Hammond admonished his co-conspirators that while they should make as many unauthorized charges to the stolen Stratfor subscribers' credit cards as possible to create "financial mayhem," deleting data and dumping sensitive stolen information on the Internet were just as important:

[Hammond]	those ccs [credit cards] and financial mayhem is definitely the most lulzy and newsworthy element of this attack
[Hammond]	and also goes with the lulzxmas theme of stealing from rich and giving to poor
[Hammond]	an equally important part is destroying their servers and dumping their user/address list and private emails
[Hammond]	with the goal of destroying the target
[Hammond]	I'm hoping bankrupcy, collapse

(Bates # 63172.)

Hammond also took charge of how the destruction of Stratfor and the public disclosure of the data he had stolen would be publicized for maximum impact. Among other things, Hammond:

- created the code that defaced Stratfor's website prior to the deletion of all of the data on Stratfor's computer network (Bates # 63197-98, 63202);
- arranged for "teasers" of limited amounts of stolen data – principally Stratfor subscribers' personal information and credit card numbers – to be published online to generate interest in the main dump of information that Hammond had planned (Bates # 63164, 63191);

- drafted "press releases" to go along with each disclosure (Bates # 63166, 63192, 63194);

- directed his co-conspirators to examine the stolen Stratfor material for information about famous or noteworthy Stratfor subscribers that could be singled out for public ridicule (Bates # 63215); and

- came up with the idea of sending spam emails to thousands of Stratfor subscribers purporting to come from a Stratfor executive and attaching a document (a "zine") that not only documented the Stratfor hack, but also contained sensitive information, including data on thousands of emails and credit cards, that Hammond had stolen as a result of cyber attacks on the websites and computer systems of three other law enforcement targets: the California Statewide Law Enforcement Association; the New York State Association of Chiefs of Police; and Special Forces Gear, a company which sold equipment to military and law enforcement personnel.[9] The document also included a claim that more than $500,000 in unauthorized charges had been made to credit cards stolen through the hacking activity. (Bates # 63166, 63170, 63202-03, 63271, 77637 *et seq.*)

On December 24, 2011, after causing his co-conspirators to hype the event on Twitter (Bates # 63205 ("Can we get them twitters going, hypin people up?")), Hammond defaced Stratfor's website and, minutes later, deleted all of the data on its computer servers – knocking Stratfor offline for the next six weeks. (Bates # 63197-99, 63205-09.) Unsurprisingly, given

---

[9] In a chat with a co-conspirator on December 13, 2011, Hammond had boasted of hacking into Special Forces Gear's website and stealing emails and customers' credit card numbers and discussed the impact of including that stolen data in the "zine," particularly because it contained personal information relating to a federal law enforcement agent:

[Hammond]	I re-owned and rooted their server
[Hammond]	and grabbed the encryption keys back again . . . as well as their massive mail spools
<~elChe>	lol
[Hammond]	dropping the CCs [credit cards] will only enhance the mayhem
[Hammond]	especially cause we got an FBI home address + card

(Bates # 63162.)

Hammond's efforts to publicize the hack, reaction in the press and online was immediate. When a Stratfor subscriber expressed outrage on a social media site, Hammond located among the Stratfor data he had stolen the subscriber's personal information, including the subscriber's credit card data, email address and home address; pasted it in a chat channel visible to his co-conspirators; noted that the credit card information was still good; and directed his co-conspirators to make fraudulent charges against it. (Bates # 63229-31 ("Yall can go ahead and ride on him.").) Finally, on December 29, after having published several teasers of stolen data, Hammond dumped online account information relating to approximately 860,000 Stratfor subscribers, as well as approximately 60,000 credit cards numbers belonging to Stratfor clients. On January 6, 2012, Hammond caused the spam email attaching the zine noted above to be sent to Stratfor clients, whose information, including email accounts, he had compromised.

C. Hammond's Other Online Attacks

Hammond's recorded online chats with the CW, evidence recovered from his laptop at the time of his arrest, and his admissions in the Plea Agreement show that Hammond has engaged in many more attempted and successful online attacks. In his Plea Agreement, Hammond admitted that, in addition to the AZDPS and the Special Forces Gear hacks noted above, in 2011 and 2012 he also attacked, stole and disseminated confidential information from websites and computer networks used by the following victims:

- the Federal Bureau of Investigation's Virtual Academy;
- Brooks-Jeffrey Marketing, Inc. ("BJM"), which maintained various law enforcement-related websites;
- Vanguard Defense Industries ("Vanguard");

- the Jefferson County, Alabama Sheriff's Office;
- the Boston Police Patrolmen's Association ("BPPA"); and
- Combined Systems, Inc.

(PSR ¶¶ 30-37.)

In addition to the foregoing, in recorded chats with the CW, Hammond bragged about attacks against the computer systems and websites of over 30 businesses, governments, and law enforcement organizations, including, among others, the Syracuse Police Department; the town of Gates, New York; "OnGuardOnline.gov," a federal website designed to promote safe, secure and responsible use of the Internet; the Lake County, Florida Sheriff's Office; and the Boston Police Department.

Hammond's laptop, which was seized at the time of his arrest while he was chatting online with the CW, also contained a wealth of evidence relating to his criminal hacking activities. Among other things, Hammond's laptop contained files that documented attacks on computer systems belonging to scores of entities, including successful cyber attacks against:

- the Federal Trade Commission and its website, as well as at least two other related consumer protection websites operated by the federal government;
- the New York Police Department's Equipment Section, including the theft of a database containing the names, home addresses, email accounts and credit card information of at least hundreds of customers of its website;
- Southern Police Equipment Supply, including its website;
- the Austin Police Retirement System, including the theft of a database containing the names, email addresses, passwords, dates of birth, and associated account numbers of at least hundreds of retired police officers; and
- Panda Security and its website, including the theft of email addresses and passwords of hundreds of Panda Security employees and users.

Indeed, an examination of Hammond's laptop revealed open terminal panels which showed that Hammond was logged into Panda Security's computer network at the very moment he was arrested.[10] Other open files on Hammond's desktop included, for example, .pdfs of tax returns belonging to innocent third parties, lists of usernames and passwords for various victim websites and servers, and an email application which showed that Hammond had live access to numerous victim email accounts that he had compromised.[11]

II. Hammond's Arrest and Indictment

On March 5, 2012, agents of the Federal Bureau of Investigation ("FBI") arrested Hammond at his residence in Chicago on an arrest warrant issued pursuant to a complaint, 12 Mag. 611, that had been filed in the Southern District of New York. The Complaint charged Hammond with conspiracy to commit computer hacking, in violation of Title 18, United States Code, Section 1030(b) (Count One); substantive computer hacking, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b), (c)(4)(B)(i) and 2 (Count Two); and conspiracy to commit access device fraud, in violation of Title 18, United States Code, Section 1029(b)(2) (Count Three).

On May 2, 2012, Superseding Indictment S1 12 Cr. 185 (LAP) was filed in the Southern District of New York. In addition to the charges in the Complaint, which all related to

---

[10] On March 7, 2012, unknown individuals – likely Hammond's criminal associates with whom he had shared his successful hack of Panda Security – defaced its website and announced that it had been hacked in retaliation for Hammond and his LulzSec co-conspirators' arrests two days before. *See, e.g.*, http://www.foxnews.com/tech/2012/03/07/ anonymous-retaliates-for-lulzsec-arrests-hacks-panda-security-website/.

[11] (Bates # 1500-1555.)

Hammond's participation in the Stratfor hack, the Superseding Indictment charged Hammond with an additional count of conspiracy to commit computer hacking for his involvement in the AZDPS hack with other members of LulzSec, in violation of Title 18, United States Code, Section 1030(b),[12] and one count of aggravated identity theft in violation of Title 18, United States Code, Section 1028A, in connection with the Stratfor hack.

III. Hammond's Guilty Plea and the Presentence Investigation Report

On May 28, 2013, Hammond pleaded guilty before Your Honor to a superseding information, S2 12 Cr. 185 (LAP), pursuant to a plea agreement with the Government. The Superseding Information, which was filed on the same day, charged Hammond with one count of conspiracy to engage in computer hacking, after having been previously convicted of federal computer hacking charges, in violation of Title 18, United States Code, Section 1030(b), in connection with Hammond's participation in the Stratfor hack.

According to the terms of the Plea Agreement, Hammond admitted to participating in eight other cyber attacks besides the Stratfor hack and stipulated that this additional criminal activity was relevant conduct to be considered by the Court at the time of his sentencing.[13] (Plea

---

[12] The Superseding Indictment also included a separate conspiracy to commit computer hacking charge against Ryan Ackroyd, Jake Davis, Darren Martyn, and Donncha O'Cearrbhail for their involvement in a group called Internet Feds, a precursor hacking group to LulzSec. Ackroyd, Davis and Martyn were also charged along with Hammond for the LulzSec conspiracy; and Ackroyd, Davis, Martyn, and O'Cearrbhail were also charged along with Hammond for the Stratfor hack with AntiSec.

[13] The eight additional hacks to which Hammond admitted participating in were each the subject of a separate FBI investigation. As a result of Hammond's admission of those hacks as relevant conduct, the Government agreed not to charge Hammond for those separate offenses. In addition, the Government agreed not to charge Hammond further based on evidence obtained

Agreement at 2-3.) Hammond stipulated that his total adjusted Guidelines offense level was 31, including enhancements based on (1) a loss of more than $1,000,000 but less than $2,500,000; (2) 250 or more victims; (3) the fact that Hammond's offense conduct involved sophisticated means; (4) the fact that Hammond's offense conduct involved an intent to obtain personal information or the unauthorized public dissemination of personal information; and (5) the fact that Hammond's offense conduct involved a computer system used by or for a government entity in furtherance of the administration of justice. (*Id.* at 3-4.) In addition, Hammond stipulated that he is in Criminal History Category IV, based in part on his conviction, in 2006 in the Northern District of Illinois, for a violation of Title 18, United States Code, Title 1030(a)(2) (computer hacking), which arose from his cyber attack on and theft of thousands of credit cards from a victim's computer system and resulted in a sentence of 24 months' incarceration to be followed by a term of three years' supervised release; and because he committed the instant offense while on probation following his conviction in 2010 in Cook County (IL) Circuit Court for mob action. (*Id.* at 4-5.) Hammond agreed that his stipulated Guidelines sentence was 120 months. (*Id.* at 6.) Finally, Hammond also agreed that neither a downward nor an upward departure from the stipulated Guidelines sentence was warranted. (*Id.*)

In the PSR, the Probation Office concurred with the offense level calculations and sentencing range agreed to by Hammond in the Plea Agreement, and recommended a term of incarceration of 120 months. (PSR ¶¶ 42-77, 111; page 28.)

---

from the laptop computer seized at the time of his arrest, or based on evidence obtained from his communications with the CW. (Plea Agreement at 2-3.)

ARGUMENT

A sentence of 120 months is warranted in this case. Hammond is a hacking recidivist who, over the course of almost a year, launched cyber attacks that harmed businesses, individuals, and governments; caused losses of between $1 million and $2.5 million; affected thousands of people; and threatened the safety of the public and of law enforcement officers and their families. In 2006, Hammond was sentenced to a term of 24 months' incarceration on a federal computer hacking charge. Undaunted by this prior conviction and sentence, shortly after completing his term of supervised release for it and while on probation for yet another conviction, Hammond began a sustained campaign during which he executed cyber attacks against the websites and computer networks of scores of victims. Hammond's history of recidivism and complete disregard for the law belies his current claim at sentencing that he will not re-engage in this same criminal conduct upon his release from prison. Moreover, Hammond's own statements prior to his arrest show that, contrary to his contentions now, Hammond was motivated by a malicious and callous contempt for those with whom he disagreed, particularly anyone remotely related to law enforcement, not a "concern[] with both transparency and privacy." (Def. Mem. at 33.) For all of these reasons, as well as for the importance of deterrence, promoting respect for the law, and providing just punishment in this case, the Government respectfully submits that a sentence of 120 months would be sufficient, but not greater than necessary, to serve the legitimate purposes of sentencing.

I. Applicable Law

As the Court is well aware, in determining Hammond's sentence, the Court must consider the factors set forth in 18 U.S.C. § 3553(a). The Court must also impose a sentence sufficient, but not greater than necessary, to comply with the purposes set forth in paragraph (2) above. *Id.*

The Sentencing Guidelines, which "should be the starting point and the initial benchmark" for sentencing, *Gall* v. *United States*, 128 S.Ct. 586, 596 (2007), take into account in a case such as this the factors stipulated to by Hammond in his guilty plea agreement such as the loss amount; the number of victims; and the sophisticated means and other specific characteristics of his offense. *See* United States Sentencing Guidelines ("Guidelines" or "U.S.S.G.") §§ 2B1.1(b)(1) and (2). The combination of these characteristics, along with his lengthy criminal history and acceptance of responsibility at his plea, results in a Guidelines range of 151 to 188 months' imprisonment. However, the applicable and stipulated Guidelines sentence is 120 months, the statutory maximum for the offense of conviction.

II. Discussion

A. The Nature and Circumstances of the Offense

The nature and circumstances of Hammond's offense support the substantial period of incarceration that is called for by the Guidelines. As set forth in the Complaint, the PSR, and the Background Section, Hammond played a central role in an extensive, deliberate, and destructive hacking campaign that caused widespread and serious harm.

The victims of Hammond's hacking included local police officers and their families, federal agencies, private companies, and thousands of private individuals. Hammond caused

substantial financial harm and emotional distress, violated privacy, and endangered public safety. As a result of his hacking activities, for example, the names, physical addresses, credit card data, and email addresses of thousands of clients of Stratfor were released and disseminated worldwide (PSR ¶ 23), resulting in approximately $700,000 of unauthorized charges on those accounts (PSR ¶ 28), and cost more than $1 million to Stratfor to repair. Brooks-Jeffrey Marketing, another of Hammond's victims, which maintains and services various law enforcement websites, suffered over $280,000 in financial loss. (*See* Letter of BJM of April 17, 2013.) Vanguard calculated over $70,000 in financial loss, and the Arizona Fraternal Order of Police, over $20,000. (*See* Letter of [redacted] dated September 26, 2013 ("[redacted] Letter"); Letter of [redacted] dated September 25, 2013 ("[redacted] Letter").)

Moreover, much of the damage Hammond caused cannot even be quantified. A retired police officer and his wife, whose unlisted home phone number was released as a result of the AZDPS hack, received hundreds of harassing phone calls for weeks after – including physical threats. (*See* Letter of [redacted] dated August 12, 2013.) Indeed, the AZDPS – Arizona's statewide law enforcement agency – had to shut down its external email server, as well as its sex offender website and its fingerprint identification system, in order to address the damage from Hammond's hack. Arizona's Amber Alert System – which broadcasts "urgent bulletin[s] in the most serious child-abduction cases"[14] – and that state's ability to track its

[14] *See* Website of U.S. Department of Justice, AMBER Alert, America's Missing: Broadcast Emergency Response, http://www.amberalert.gov/.

aircraft and helicopters were also impacted by Hammond's cyber attack. (*See* Letter of [redacted], Director, AZDPS, dated August 23, 2013.)

As a result of Hammond's related hack of the Arizona Fraternal Order of Police, the personal information, including the home addresses, of hundreds of active and retired law enforcement officers was disseminated online, and his hack of Vanguard released, among other things, the entire personal financial information of one of Vanguard's officers, all of which raised significant concerns about safety, privacy violations, and financial fraud for hundreds of individuals. (*See* [redacted] Letter; [redacted] Letter.)

Hammond played a leading role in all of these hacks, as well as other similar hacks described in the Background Section above, due mainly to his hacking experience and ability, as well as his relentlessness in identifying and attacking targets, particularly those tied to law enforcement. By his own account, his extensive involvement in computer hacking dates back at least a decade (Def. Mem. at 17), and his criminal hacking to at least 2005 (PSR ¶ 61). Indeed, it was Hammond himself who brought the AZDPS hack to LulzSec, his first foray with that hacking organization, bragging to the CW, "this time we have some high profile shit," uploading "a sample pdf" containing what appeared to be the name, phone number, and an e-mail address of an Arizona detective as evidence of what he had stolen, and then boasting later, "anyway, there's a LOT more where that came from."[15] He then spent a few days going through the stolen material on his own, periodically sharing additional samples with his co-conspirators and the CW

[15] (Bates # 78130-31.)

until he was ready to share the entire set of data, and he also contributed to drafting the press releases and strategized about the publicity campaign and release itself.[16]

Although Hammond does not appear to have initiated the Stratfor hack, he played a central role in that attack as well, in bringing it to fruition. In his submission, Hammond makes much of the CW's role in introducing Hammond to the hacker "hyrriiya" after the CW learned that hyrriiya claimed to have hacked into Stratfor. (Def. Mem. at 20-21.) Hammond elides over his own key role – which was to take over the hack from hyrriiya and carry it through to its successful completion. Indeed, about 20 minutes after the CW introduced them, Hammond informed the CW, "[i]t looks like he [hyrriiya] needs help breaking into their [Stratfor's] servers."[17] And Hammond moved quickly to do what hyrriiya could not – completely penetrate and take over Stratfor's computer network. Hammond's criminal expertise and focus were instrumental to the success of the Stratfor hack.

Hammond played a similar central role in numerous other hacks, including those to which he pled, as well as a number of others, as described in greater detail in the Background Section. Notably, he worked on many of these on his own, as the evidence on his hard drive demonstrates – obtaining access to victim computer networks through vulnerabilities that he identified and that he knew how to exploit, and then stealing data, storing it on his hard drive, and going through it in detail before sharing it with others for release.

---

[16] (Bates # 78128-78244.)

[17] (Bates # 67014.)

Hammond's attempts to deflect blame or obfuscate his criminal activity are without merit. Among other things, Hammond claims in his sentencing submission that the CW actually participated in the Stratfor hack – rather than gathering information about it for law enforcement – by "providing servers for the storage of information and creating chatrooms to facilitate discussions." (Def. Mem. at 21 and note 17.) This claim mischaracterizes the CW's role. As explained in the Complaint, the CW, at the direction of the FBI, provided to Hammond and his co-conspirators a server, which Hammond and his co-conspirators used to store the data they stole from Stratfor.[18] (*See* Compl. ¶ 18j.) As a result of the FBI's control of this server, the FBI was able to mitigate the harm by, for example, notifying credit card companies about the compromised cards. The FBI's control of access to this server also would, and did, provide substantial evidence as to Hammond's identity and role in the attack. Similarly, the CW created chat rooms for Hammond and his co-conspirators at the direction of the FBI, which monitored the chats, gaining valuable intelligence about the hack which it used to notify Stratfor and credit card companies as the hack developed, as well as powerful evidence of Hammond's criminal activity.[19]

---

[18] Indeed, as Hammond is aware, an encryption key that the CW passed to Hammond so Hammond could access this server was found on Hammond's hard drive, conclusively demonstrating that Hammond had accessed this server himself.

[19] In an addendum to his sentencing submission, Hammond discusses additional hacks and conduct that he claims "provide the contextual framework for the Court's overall consideration of [his] intentions and motivation." (Def. Exh. H at 1.) Specifically, Hammond alleges that the Government was "using [Hammond] to collect information regarding the vulnerabilities of foreign government websites and in some cases, disabling them." (*Id*. at 2.) Hammond apparently reaches this dramatic conclusion based in part on a partially-redacted online posting by an anonymous individual who claimed to have hacked a foreign government at the behest of

B. History and Characteristics of the Defendant

Hammond's history and characteristics – in particular his unrepentant recidivism – also support a sentence of 120 months. Moreover, Hammond's claim now that his sole intent in engaging in the instant offense conduct was to serve the public good is false. As set forth below, the evidence shows that he was in fact engaged in a campaign of online sabotage, which damaged numerous websites and resulted in the unauthorized disclosure of the personal and financial information of thousands of individuals. Having previously received leniency in connection with his prior federal sentence for computer hacking, he is entitled to none in this case.

The defendant has an almost unbroken record of criminal offenses that demonstrate a total lack of respect for the law. As noted in the PSR, this prior criminal history includes, among others, a plea of guilty to criminal damage to property in 2003 (PSR ¶ 59), and convictions for battery in 2004 (PSR ¶ 60), disorderly conduct in 2006 (PSR ¶¶ 64-65), and mob action in 2009 (PSR ¶¶ 65-66), as well as multiple violations of supervised release, parole and probation (PSR ¶¶ 62, 64, 66, 68) and other arrests for disorderly conduct, contempt of court, and criminal trespass, among others (PSR ¶¶ 70, 72, 74, 75, 76, 77). Even more significantly, that prior criminal history also includes a federal conviction, in 2006, for the same offense – and

---

the CW. These claims are baseless. While the CW and Hammond did discuss vulnerabilities of foreign websites (among others), in fact, the FBI notified foreign governments about this activity and the vulnerabilities in their websites after Hammond was arrested and the CW's role could be revealed without harming the investigation so they could take appropriate remedial action. In any event, even if Hammond's allegations were true, which they are not, they do not bear on any issues relevant to sentencing.

essentially the same conduct – for which he is being sentenced here: the defendant hacked the website of an organization he disagreed with politically and obtained information such as the credit card numbers, home addresses and other identifying information of its members and customers. (PSR ¶ 61.) As here, he intended to make unauthorized charges using those stolen credit cards.[20] Hammond began engaging in his most recent hacking spree while serving a term of probation. (PSR ¶ 68.) Given that record, the Probation Office correctly notes in the PSR Hammond's "propensity to continue to commit crime," concluding that "[t]here is no information in his record that would suggest that he will not continue to recidivate." (PSR, page 29 ("The defendant's criminal record shows his disdain for the law as he has been cited for several violations while serving terms of supervision, along with two notable sanctions while housed at the Bureau of Prisons.").)[21]

Hammond argues that he is entitled to leniency because he was motivated by altruism. (Def. Mem. at 28.) That claim is false. Hammond's claim now that he was actually only engaged in a campaign of "civil disobedience" to expose government and corporate malfeasance is overwhelmingly contradicted by his own statements at the time of these hacks. Those statements to his confederates, long before he was arrested and when he did not expect to be caught, more likely reflect his true nature and intent rather than his post-hoc rationalizations now that he is actually being called to account for his actions.

---

[20] *See* Transcript of Sentencing, Dec. 7, 2006, Exhibit A (Bates # 000180 – 000222), at 15-17 ("Sentencing Tr.").

[21] Hammond violated Bureau of Prison rules by testing positive for marijuana and disobeying an order, resulting in sanctions including disciplinary segregation and loss of commissary, phone, and visiting privileges. (PSR ¶¶ 8-9.)

And what those statements generally demonstrate is that Hammond repeatedly expressed his goals to wreak havoc, damage law enforcement and anyone linked to it, and steal and disseminate financial information such as credit cards. Hammond bragged to his co-conspirators that he had "a three punch knockout plan" with regard to the stolen AZDPS data, and described one set of those materials as follows: "the last one was focused more on confidential documents/this one focuses more on personal email accounts, girlfriend pics, dirt and scandals."[22] In discussing the Stratfor hack, Hammond had extensive discussions about exploiting the stolen credit card information, including what to purchase with them,[23] and reveling in the chaos that he imagined would ensue. Hammond's destructive goals are evident not only in his discussions about AZDPS and Stratfor but also many others. For example, Hammond bragged to the CW about the information he had stolen from Special Forces Gear:

> [Hammond] the password list is fucking huge, and includes many .mil and .govs
> . . .

---

[22] (Bates #078241-42.) A bit later, in the same chat, referring to one specific AZDPS employee, Hammond proposed, "if we drop AZ stuff on wednesday, we might want to pull some other prank, like change the AZDPS facebook group, his online dating profile or something silly."

[23] For example, in a chat on December 19, 2011, Hammond said to his co-conspirators:

> [Hammond] I was thinking we order some servesr with them stolen CCs
> [Hammond] lots of servers with big hard drives
> [Hammond] and make four or five mirror .onions with them . . .
> . . .
> <~el che> getting servers with CCs
> [Hammond] it may be till the end of the mnth before the cc owner recognizes the bad charges

(Bates # 63171.)

[Hammond] furthemrore

[Hammond] there are fuckloads of CCs

[Hammond] with expiration dates and addresses, but no CVV2s[24]

[Hammond] if we can utilize this, we should, otherwise, we could just dump itand watch the mayhem unfold.[25]

Similarly, about the BPPA hack, he told the CW: "*gotta target the officers individually* . . . i'll put more work in later to see if we can destroy the site/we can do some cheesy defacement now by using their admin panel but it's limited/its' the only site on the server. . . ."[26] Hammond expressed the same attitude about the hack into Combined Systems:

[Hammond] back on that combinedsystems box

[Hammond] there may be some good shit here

[Hammond] I dumped the db [database] again and saw more customers

[Hammond] some good, good customers

. . . .

[Hammond] but here is the paydirt friend . . .

This last boast is followed by Hammond's "paydirt": pages of what appear to be names, email addresses, physical addresses, and credit card numbers of numerous individuals, including police officers.[27]

---

[24] "CVV2s" refers to "card verification value," generally a three-digit code that typically appears on the reverse side of credit cards, as an anti-fraud measure often used for online transactions to verify that the credit card user is in possession of a valid credit card at the time of the transaction.

[25] (Bates # 67346.)

[26] (Bates # 67350 (emphasis added).)

[27] (Bates # 67584-67589.)

Hammond's own statements, while he was plotting and committing these attacks, demonstrate that his goals at the time were essentially to cause "mass mayhem" by destroying websites of entities he disliked, particularly related to law enforcement, and revealing stolen private information such as physical addresses, personal emails, and credit card data belonging to swaths of people remotely associated with those entities. Against this evidence, Hammond's claim now that his various law enforcement targets "were significant to [him] as a way of protesting police brutality, overly aggressive and militaristic anti-immigration laws and practices, and the governments' use of drones, tear gas and other weapons abroad" (Def. Mem. at 21) is, at best, beside the point.

There is nothing about this case that supports his argument for leniency now. It is notable that he has already been the beneficiary of leniency for his prior conviction, and the sentencing proceeding in that case is instructive. Hammond and his counsel argued for leniency then based on his youth and immaturity (he was 19 at the time), the absence of any malicious motive, and the fact that he did not actually make unauthorized charges on the stolen cards. [28]

---

[28] *See, e.g.*, Sentencing Tr. at 13 ((Hammond's counsel) ("In this case, he made a mistake. This one time, he took financial information that he shouldn't have had and did possess it. On the balance of that . . . he had that in his possession for a substantial period of time and did not benefit himself financially in any way. He did not steal from anyone.")); Sentencing Tr. at 17 ((Hammond's counsel) ("Mr. Hammond is in the possession of a very powerful, powerful power . . . . And I think that because of his age, because of the fact that, you know, he didn't show the responsibility that he needed to show utilizing that skill . . . . It's like bazookas in the hands of a child."); Sentencing Tr. at 19 ((Hammond) ("Although I clearly broke the law, my motivations were not to steal or to bring harm to anybody, physically or financially. . . . I was motivated out of altruism, not out of self-interest, not out of personal financial goals.").)

And the Court did substantially depart from the Guidelines, imposing a sentence of 24 months.[29] The sentencing judge explained his sentence to Hammond:

> I believe you when you say that you have learned. I think, also, that after you're done serving your sentence, I would be willing to believe you if you told me that you understood precisely how damaging the democratic discourse of what you did is. I don't know that you fully understand that now. I concede that you fully understand what you did was wrong.
>
> I believe that a 41-month sentence is too long in this particular case. It is, from my perspective, out of line with other sentences for computer hacking offenses, particularly those done out of unguided malice, a desire to wreak havoc, which motivates many hacking offenses, and those done for profit, and I suppose you could add to that those done to perpetrate particular harm against the named person. Yours, in many respects, is on the low end of the scale, but it's not at the bottom of the scale, because the prosecutor was right, that the damage you did, more precisely the threat of what you did, is damaging the democratic discourse, your side's as well as the other.[30]

There are of course notable differences between his prior federal conviction and this offense: that case involved one website and actual loss of $1,658, and the defendant did not in the end follow through with his plan to use the stolen credit cards.[31] Unfortunately, though, Hammond did not learn, or at least not apparently anything positive, from the leniency shown to him then. In June 2011, barely a month after his term of supervised release ended (PSR ¶ 63), Hammond had already begun the conduct to which he pled guilty here: he approached the CW with his hack into the AZDPS, thus embarking on a hacking spree that dwarfed his 2006 offense

---

[29] The applicable guidelines range was 41 to 51 months. (Sentencing Tr. at 36.)

[30] Sentencing Tr. at 36-37.

[31] Sentencing Tr. at 3-4, 24.

in scope, in volume, in the number of victims, in the losses caused, and in the damage done – not to mention that, this time, hundreds of stolen credit cards were in fact disseminated and used.

Hammond was given a substantial sentencing break when he committed his first federal offense. At the time, the judge explained his decision to be lenient by noting that Hammond's crime was distinguishable from those hacking offenses which warranted substantial Guidelines punishment, pointing in particular to "those done out of unguided malice, a desire to wreak havoc, which motivates many hacking offenses."[32] Rather than heed the Court's message, or even apparently reflect much on its leniency, Hammond then proceeded to undertake the same conduct the Court had cautioned against – but on a much greater scale – launching an online campaign of cyber attacks characterized by "unguided malice [and] a desire to wreak havoc." Hammond's history and characteristics fully support a sentence of 120 months.[33]

C. The Need to Promote Respect for the Law, to Ensure Just Punishment, and for Deterrence in this Case

There is a critical need in this case to promote respect for the law and ensure just punishment. Hammond's plea for a sentence of time served, that is, four months less than the 24-month sentence he received for his prior conviction (Def. Mem. at 34), should be rejected.

---

[32] Sentencing Tr. at 36.

[33] As Hammond correctly notes in his sentencing submission, the Government is unaware of any evidence that he personally used the stolen credit cards or that he was motivated by personal financial gain. (Def. Mem. at 21.) Similarly, the Government has no reason to doubt that Hammond has been helpful and charitable to others, as many of his supporters attest, or that he also was motivated to contribute to the public good. In the Government's view, these positive characteristics are significantly outweighed by the widespread harm he caused to so many, financially and otherwise.

After the leniency he received previously, he immediately re-engaged and expanded upon his prior offense – resulting in exponentially greater damage to thousands more victims. Hammond's assertion that he is "not without regret" that "private information of innocent parties was released to the public, and [for] any consequences suffered as a result of that breach of privacy" (Def. Mem. at 28) rings hollow, especially against his repeated contemporaneous expressions of the intent to cause precisely that harm on a mass scale. More leniency now would hardly serve as just punishment for a repeat offender nor would it serve as deterrence either to Hammond or to others who may be inclined to undertake similar activities. Hammond was already given a second chance to demonstrate that he could lead a law-abiding life. Instead, having been given leniency, he chose to dramatically escalate his prior offense in scope and consequences. As a result, he caused financial harm and emotional distress, violated privacy, and jeopardized public safety, to various entities and numerous individuals he had never met – in other words, he wreaked havoc, just as he hoped to. His conduct now deserves the strongest possible condemnation.

The factors that the Court is to take into account indicate that a sentence of 120 months is appropriate and warranted, principally due to the seriousness of Hammond's offense, and the substantial harm he caused; his history and characteristics, in particular his recidivism; and the need for deterrence and just punishment.

CONCLUSION

For the foregoing reasons, the Government respectfully submits that a sentence of 120 months, the stipulated Guidelines sentence and the applicable statutory maximum, is sufficient, but no greater than necessary to meet the goals of Section 3553(a).

Dated: New York, New York
November 12, 2013

Respectfully submitted,

PREET BHARARA
United States Attorney for the
Southern District of New York

By: _____/S/_____
Thomas Brown/Rosemary Nidiry
Assistant United States Attorneys
Tel.: 212-637-2194/1063

CERTIFICATION OF SERVICE

I hereby certify that a copy of the Government's Memorandum of Law With Respect to Sentencing filed in this matter was served on:

Susan G. Kellman, Esq.
Law Offices of Susan G. Kellman
25 Eighth Avenue
Brooklyn, New York 11217
email: kellmanesq@aol.com

by electronic mail on the 12th day of November 2013

/S/
Thomas Brown
Assistant U.S. Attorney